

DEPARTMENT OF HEALTH & HUMAN SERVICES  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard, Mail Stop N1-19-18  
Baltimore, Maryland 21244-1850



**Office of Information Services**

---

# Enterprise User Administration

## Users Guide

Version 1.1

## Table of Contents

Introduction.....	2
New User Requests .....	2
User Change Requests .....	2
CMS Userid Certification Requirements .....	3
EUA PassPort .....	3
Installation of PassPort .....	4
Logging on to PassPort .....	4
PassPort Home Screen .....	5
PassPort Certification Screens .....	6
Managing Passwords .....	11
Using PassPort to Manage Passwords .....	11
Setting Up Challenges.....	13
Logging on to PassPort Without a Password.....	15

### Introduction

This guide provides information on the Enterprise User Administration (EUA) system used by the Centers for Medicare & Medicaid Services (CMS) and the CMS Data Center (CMSDC). The guide discusses the role of EUA in userid and password management, and provides instructions for installation and operation of EUA support products available to the user.

EUA is a system used by CMS to manage enterprise userids and passwords. It allows for centralized administration of userids on the entire CMS enterprise including the mainframe systems, mid-tier devices such as AIX or SUN systems, network operating systems such as Netware or Windows, and database platforms such as Oracle, Sybase, and MS SQL. The system utilizes online data to automate the approval process for access requests, and provides logging and auditing support.

EUA only manages resources resident at the CMSDC and at CMS Web sites. Therefore, it does not control remote dialup access userids provided by AGNS, or Health and Human Services (HHS) provided resources such as the Integrated Time and Attendance System (ITAS) and the new Email system. Users need to manage those userids and passwords through mechanisms provided in those environments. EUA also does not manage local IDs created in application tables. Users need to contact application owners for instructions on how these can be maintained.

### New User Requests

The process for new users requesting access to CMS resources requires submission of a signed paper request form. For CMS employees, the new user provisioning process is handled by the agency personnel department. New contractor personnel need to complete the Application for Access to CMS Computer Systems Form available at

<http://www.cms.hhs.gov/mdcn/hdcidform.asp>

The contractor should forward the signed form according to the instructions provided with it.

### User Change Requests

All users may submit change requests by sending an email to the RACF Group Administrator (RGA) responsible for their userids. The RGA will enter the request into EUA, where it will be routed to the appropriate approving authorities. Contractors must immediately notify CMS upon termination of any employees who hold CMS userids.

## **CMS Userid Certification Requirements**

CMS requires everyone who has an enterprise userid to complete an annual certification of their access needs, and to take a security Computer Based Training (CBT) course. Users who do not complete these tasks by their certification due date will have their access rights revoked.

Six weeks prior to the due date, each user receives an email message notifying them of the need to certify and complete the CBT. The email contains Web browser links to the EUA PassPort application, and to the CBT Web pages. A printed letter is sent to those users who do not have email addresses on file with CMS. Some external users may not be able to access the PassPort and CBT services. These services are not available from the Internet, but are accessible over the Medicare Data Communications Network (MDCN). The user notifications also include instructions on using the existing paper based certification process, and an alternate CBT process.

Two weeks before the due date, a reminder notice is sent to those users who have not completed the certification requirements. If the users do not certify before the deadline, their access rights are revoked.

Users whose access rights have been revoked due to non-certification need to request reinstatement by sending an email to [CMSEUA@cms.hhs.gov](mailto:CMSEUA@cms.hhs.gov). If the user is a CMS employee, the request should come from their supervisor. For all other users, the RGA or project officer for the contract should send the request. Reinstatements will only be granted for a two week period. If the user does not complete the certification within the two week period, the userid will again be revoked.

Note that both the paper and electronic certifications require CMS approval before the user is considered certified. Please allow some time for this approval process, i.e., don't wait until the day before expiration to submit the certification request.

## **EUA PassPort**

PassPort is a Web based application used to provide users with an interface to EUA. The two principal uses of PassPort are for the annual user certification of access requirements, and password management. Use of PassPort is not required by CMS, but its capabilities should simplify the userid management process for users.

## Installation of PassPort

Since PassPort is a Web based application, no user installation is needed. The only software needed on the user workstation is a Web browser such as Internet Explorer or Netscape. CMS employees have an icon for PassPort on their desktops. The icon



contains the PassPort logo:

Other users can create a desktop icon for PassPort. Instructions for creating icons are available in the CMS Remote Access Guide, available at

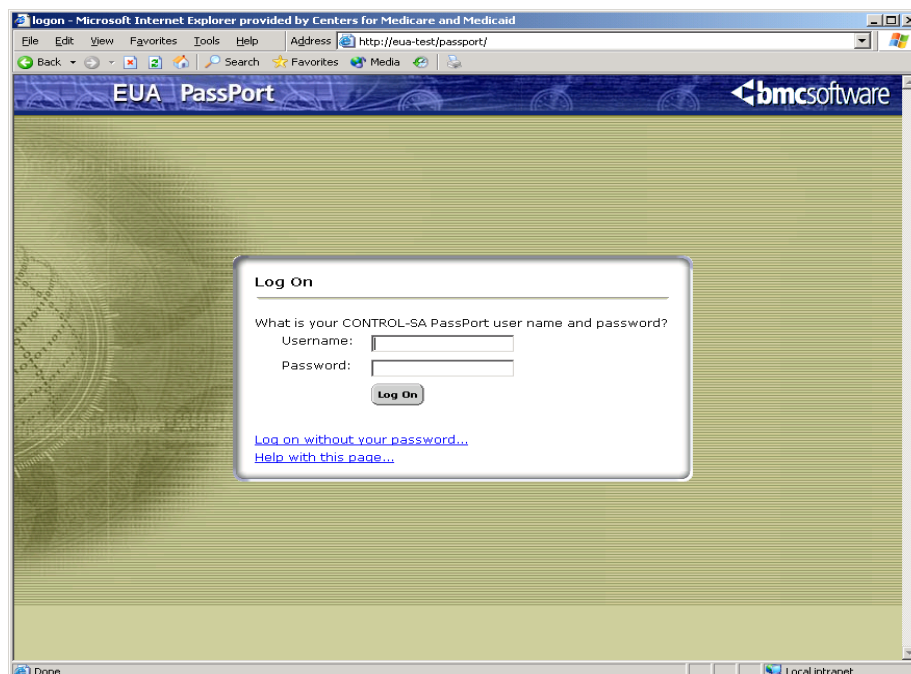
<http://www.cms.hhs.gov/mdcn/cmsremoteaccessguide.pdf>

## Logging on to PassPort

PassPort is accessed by entering the following URL in the Web browser:

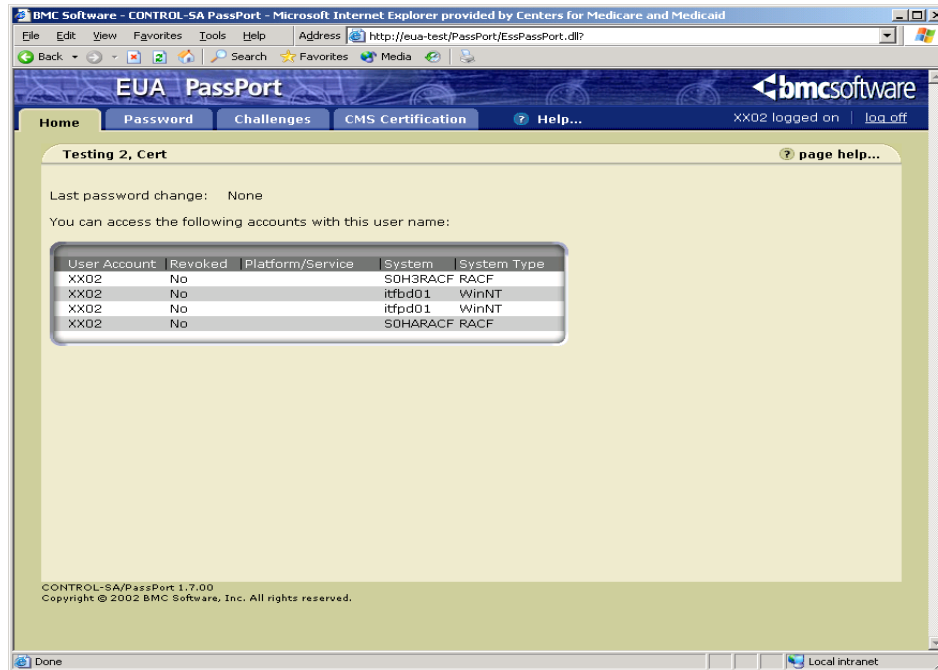
<https://158.73.79.141/passport>

The user then enters their CMS enterprise userid and password on the following screen:



## PassPort Home Screen

Upon successful login to PassPort, the user is presented with the home screen:



This screen lists the systems on which the user has accounts, and the status of those accounts.

## PassPort Certification Screens

Selecting the CMS Certification tab brings up the following screen:

**CMS Certification As of Date : 2/19/2004**

User Details	
User ID	XX04
User Name	Testing 4, Cert
Common Name	
Telephone Number	410-786-5801
Company Name	
Company Phone Number	
Address	
Mail Stop	n1-19-18
Desk Location	n1-19-17
Email Address	itfadmin@cms.hhs.gov

To change your user information, contact your RGA. [Click here to find the RGA for your Organization](#)

System Access Status				
OK	DUE	TEMP	PENDING	DUE DATE
				01/31/2004

To Certify your System Access click here : [Update System Access](#)

CBT Status			
OK	DUE	TEMP	DUE DATE
			01/31/2004

The screen has three sections. The first section presents the user details, as recorded in EUA. If any of this information is incorrect, the user's RGA should be contacted. The link "[Click here to find the RGA for your organization](#)" is available to assist users in finding their RGA.

The second section displays the System Access Status. In this example, the user is due for certification, and the due date is 1/31/2004. The third section displays the security CBT status. The example shows this as "DUE", with a due date of 1/31/2004.

## EUA Users Guide

To certify system access, the user should click on Update System Access, at which time the following screen is presented:

**Certify System Access**

1. Review each System Access that is presented
2. For each System Access select either keep or delete
3. Select Certify when you are finished or select Cancel to quit
4. Maximum Length of comment field must be 235.

**Keep** : Select to retain system access to perform your current job function  
**Delete** : Select to remove system access if access is no longer required

KEEP	DELETE	SYSTEM ACCESS	DESCRIPTION
<input type="radio"/>	<input type="radio"/>	Default Groupwise	CMS GroupWise Email
<input type="radio"/>	<input type="radio"/>	TSO_D_User	TSO- Development Access
<input type="radio"/>	<input type="radio"/>	TSO_P_User	TSO- Production Access

Comments :  0

This screen summarizes the accesses the user holds. The user is given the opportunity to select “KEEP” or “DELETE” for each access. The comments box may be used for any comments the user wishes to provide.

**Certify System Access**

1. Review each System Access that is presented
2. For each System Access select either keep or delete
3. Select Certify when you are finished or select Cancel to quit
4. Maximum Length of comment field must be 235.

**Keep** : Select to retain system access to perform your current job function  
**Delete** : Select to remove system access if access is no longer required

KEEP	DELETE	SYSTEM ACCESS	DESCRIPTION
<input checked="" type="radio"/>	<input type="radio"/>	Default Groupwise	CMS GroupWise Email
<input checked="" type="radio"/>	<input type="radio"/>	TSO_D_User	TSO- Development Access
<input checked="" type="radio"/>	<input type="radio"/>	TSO_P_User	TSO- Production Access

Comments :  44



When the user has made a selection for each access, “Certify” is selected. The user is then presented with a Privacy Act statement:

The screenshot shows a web browser window titled "Certify System Access - Microsoft Internet Explorer provided by Centers for Medicare and Medic...". The main content area has a yellow background and contains the following text:

*Please click the button on bottom of this window to continue*

**PRIVACY ACT ADVISORY STATEMENT**

**Privacy Act of 1974, P. L. 93-579**

The information on this site is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's (formerly HCFA's) computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnish on this form will be maintained in the Individuals Authorized Access to the Centers for Medicare & Medicaid (CMS) Data Center Systems of Records and may be disclosed as a routine use disclosure under the routine uses established for this system as published at 59 FED. REG. 41329 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

Collection of the Social Security Number (SSN) is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in delaying the processing of this request.

**SECURITY REQUIREMENTS FOR USERS OF CMS's COMPUTER SYSTEMS**

This statement is the same as the one on page 2 of the Application for Access to CMS Computer Systems Form, previously signed by the user. Scrolling down to the bottom of the screen reveals the Agree and Decline buttons:

The screenshot shows the same web browser window, but with the content scrolled down. The main content area has a yellow background and contains the following text:

*someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions.*

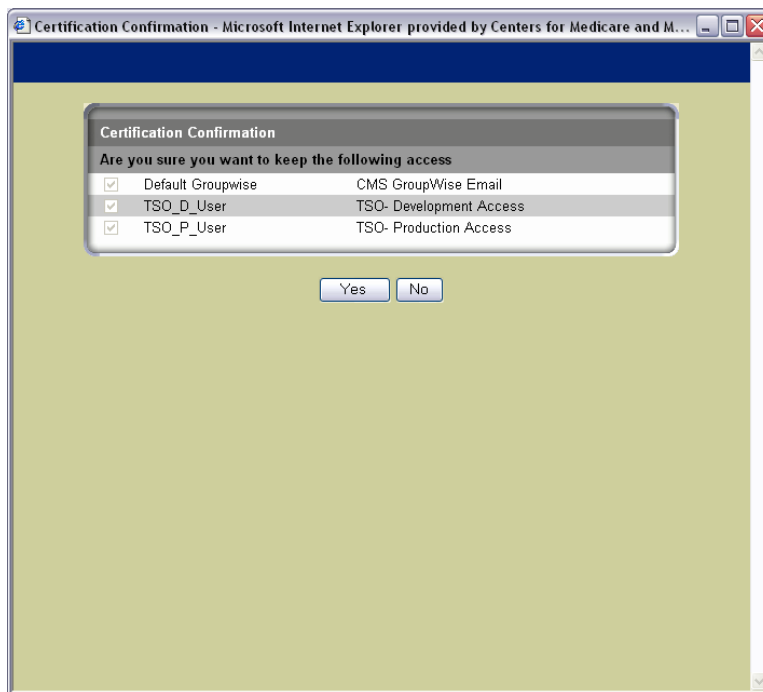
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

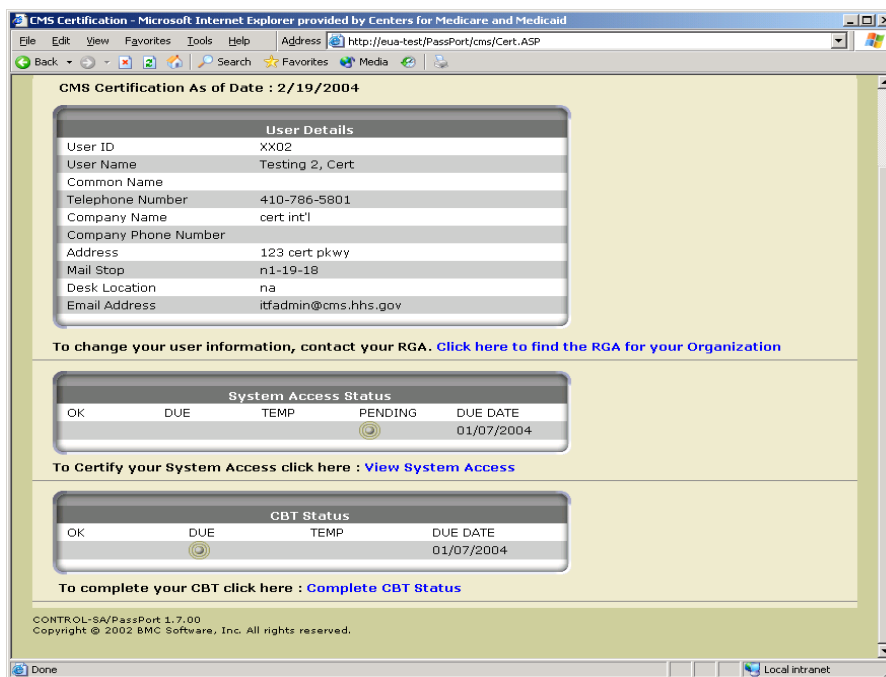
If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to your component's Information Systems Security Officer.

## EUA Users Guide

The user should click on Agree, at which time the following confirmation screen is displayed:



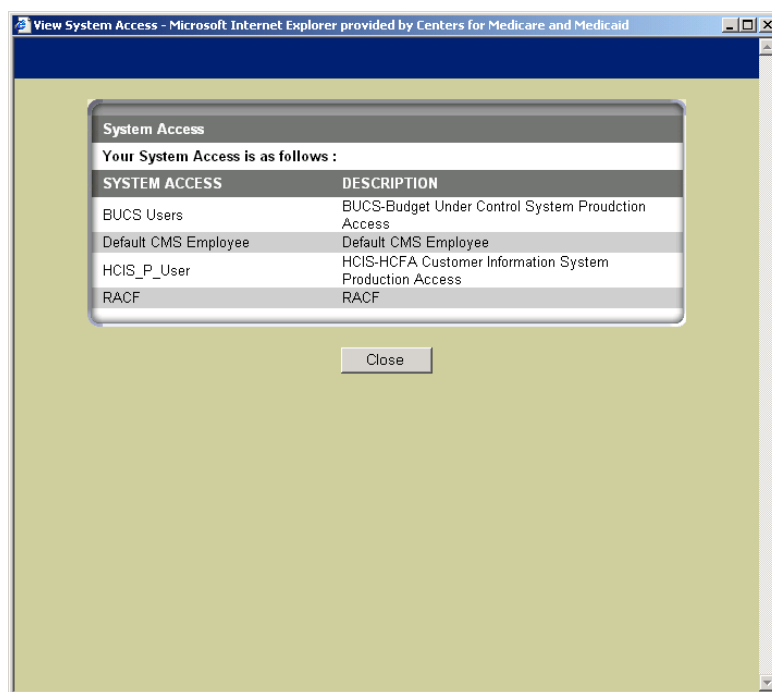
Selecting "Yes" completes the certification process for the user. At this time, the Certification screen changes the status to "PENDING":



Notice that “Update System Access” has been changed to “View System Access”. The status is now set to “PENDING”. It will remain in this state until the certification has been approved by CMS, at which time the status will change to “OK”.

The “Complete CBT Status” link can be selected when the user is ready to take the security CBT. Upon completion, the status will not immediately change to “OK”. The status update process for the CBT takes 24 hours. Users are not considered completely certified until both the System Access Status and the CBT Status are set to OK.

Selecting the “View System Access” link will present the user with a summary of accesses:



Users can view their list of accesses at any time, not just during the certification process.

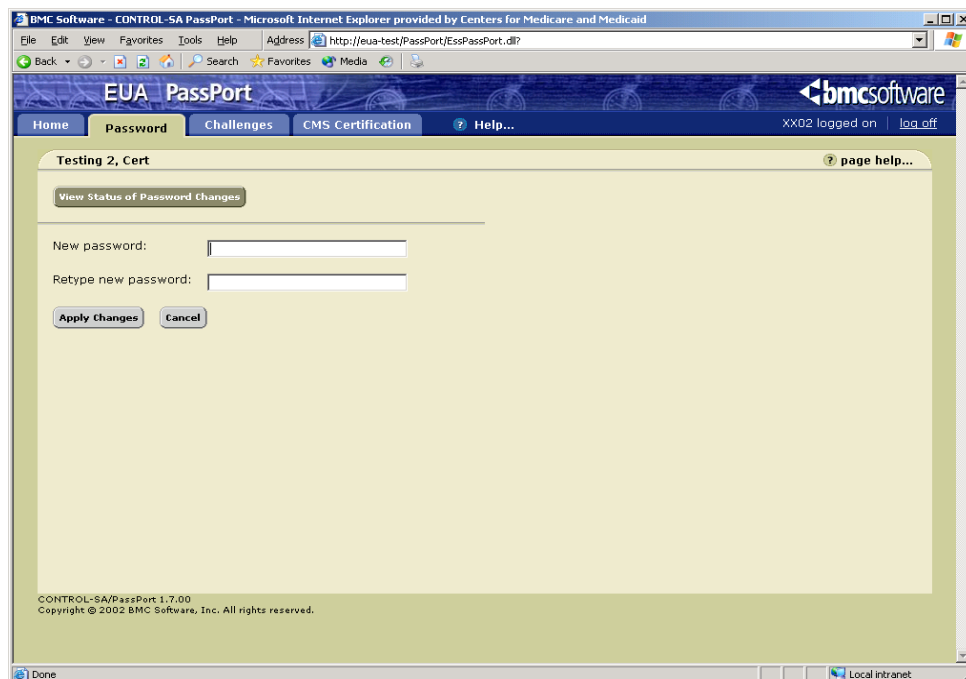
## Managing Passwords

The CMS processing environment is diverse. There are hundreds of applications hosted on a variety of platforms and servers. In an effort to reduce complexity for the users, CMS has instituted Password Propagation. This is not exactly the same as Password Synchronization. In synchronization, the systems ensure that passwords are the same on all accounts. With password propagation, changes are done natively on each platform, and password interception logic on some platforms causes the password change to be propagated to all others. This means that a user can change the password on a database platform, such as Oracle or MS SQL, and that change will not affect other platforms. CMS has ensured that password changes on platforms used for initial login, namely the mainframe, Windows NT and Active Directory, Remote Desktop (Metaframe), SUN and AIX, will be propagated to all other environments, including database platforms. As long as users change their passwords on one of these initial entry platforms, or use PassPort to change their passwords, all platforms will have the same password!

Note that a password change on the Novell Netware CMS LAN environment is synchronized to Active Directory, and will therefore be propagated to all other platforms. This means that changes to CMS employees' LAN passwords will result in change on all other platforms.

## Using PassPort to Manage Passwords

PassPort can be used to manage users' passwords. Selecting the Password tab on PassPort displays the following screen:



## EUA Users Guide

The user can then type the new password, retype it for confirmation, and select “Apply Changes”. At this time, the screen will show the following:

The screenshot shows the 'EUA PassPort' web application in a Microsoft Internet Explorer browser. The user is logged in as 'L11A'. The page title is 'LITTLE, ANNE M'. The main content area displays a green checkmark and the message 'Your change request has been submitted.' Below this, there are two input fields for 'New password:' and 'Retype new password:'. At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel'. The footer of the page indicates 'CONTROL-SA/PassPort 1.7.00 Copyright © 2002 BMC Software, Inc. All rights reserved.'

The status of the changes on the various platforms can be viewed by selecting “View Status of Password Changes”:

The screenshot shows the 'EUA PassPort' web application in a Microsoft Internet Explorer browser. The user is logged in as 'L11A'. The page title is 'LITTLE, ANNE M - Status of Password Changes'. The main content area displays a 'Back to change Password' button. Below this, a message states: 'The following table displays the account status from the last CONTROL-SA/PassPort password change request.' A 'Refresh Data' button is located above a table. The table has five columns: Date, Time, User Account, Platform/Service, and Status. It contains four rows of data, all showing 'Successful' status.

Date	Time	User Account	Platform/Service	Status
05/04/04	13:49:15	L11A		Successful
05/04/04	13:49:16	L11A		Successful
05/04/04	13:49:16	L11A		Successful
05/04/04	13:49:17	L11A.prt.NB.CO.HCFA		Successful

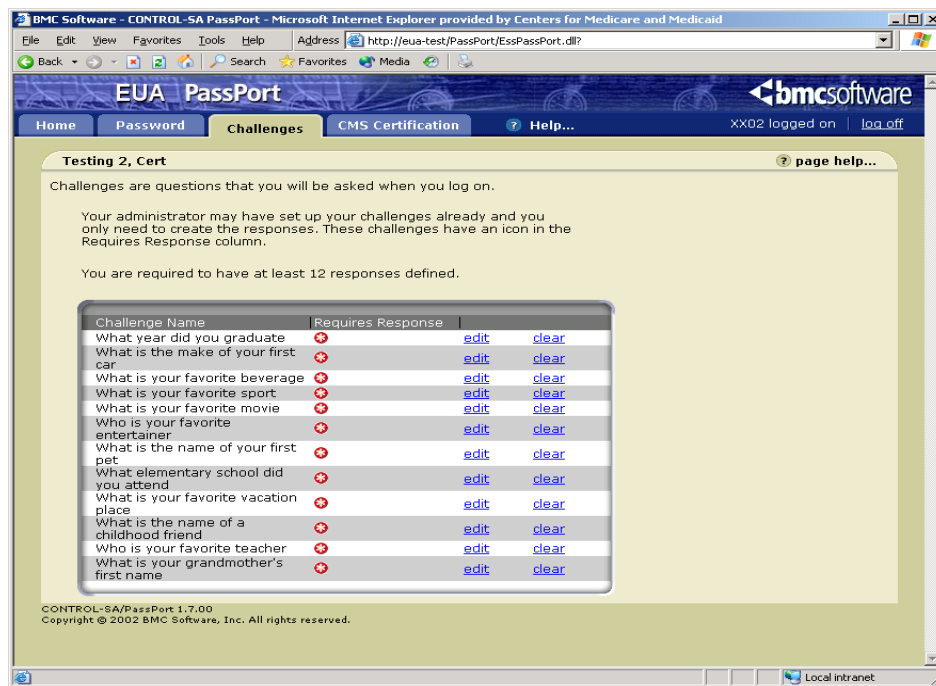
The footer of the page indicates 'CONTROL-SA/PassPort 1.7.00 Copyright © 2002 BMC Software, Inc. All rights reserved.'

The display shows the status of the password change for all accounts. The user should wait until the status is “Successful” before attempting to log on with that account.

Use of PassPort is optional. Users who cannot use PassPort, or do not wish to use it, can change their passwords when challenged by the platform and still have the change propagated to all other platforms.

## Setting Up Challenges

PassPort can also be used by users who have forgotten their passwords, or who have been revoked by mistyping their passwords. In order to utilize this feature, users need to set up challenges that can be used to authenticate them prior to password reset. This is done by selecting the “Challenges” tab:



The screen contains a list of challenges for which responses are needed. To establish a response for a given challenge, the user selects “edit”.

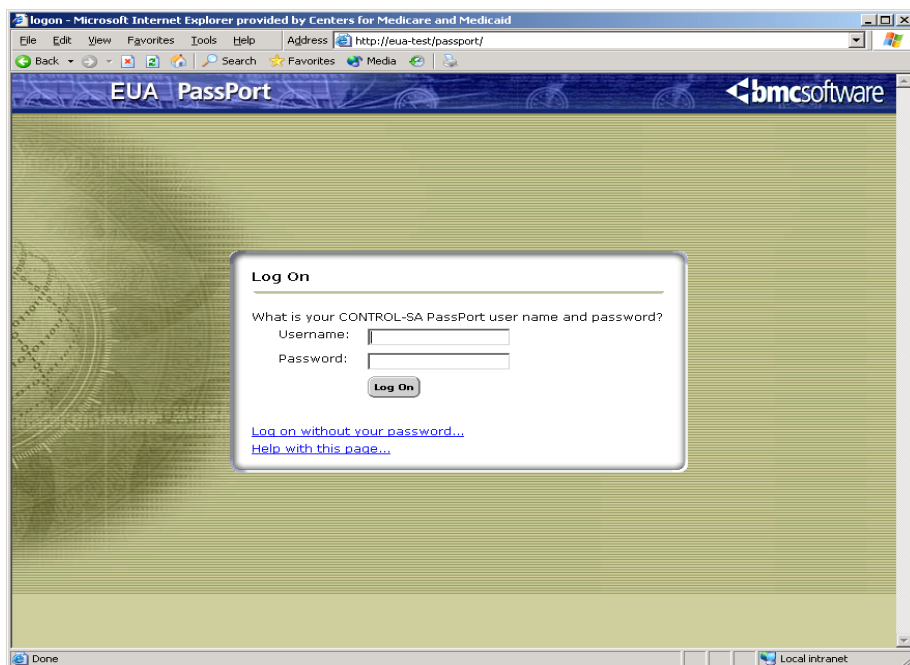
This brings up the “Edit Challenge” screen:

The screenshot shows a web browser window titled "BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid". The address bar shows "http://eua-test/PassPort/EssPassPort.dll?". The browser's menu bar includes File, Edit, View, Favorites, Tools, Help, Address, Search, Favorites, and Media. The application's navigation bar has links for Home, Password, Challenges, CMS Certification, and Help... The user is logged in as "XX04" with a "log off" link. The main content area is titled "Testing 4, Cert - Edit Challenge" and includes a "page help..." link. A "Back to Challenges" button is at the top left. Below it, a text box explains: "Challenges are questions that you will be asked when you log on. To create or change your response to this challenge, type the response to the question, then click the 'Apply Changes' button. Your response will be updated in the list below." The challenge question is "What elementary school did you attend". The "Response:" field contains six asterisks. The "Retype Response:" field also contains six asterisks, with a note "(minimum 4 characters)". At the bottom of the form are "Apply Changes" and "Cancel" buttons. The footer of the application area reads "CONTROL-SA/PassPort 1.7.00 Copyright © 2001 BMC Software, Inc". The browser's status bar at the bottom shows "javascript:doSub('OnUpdateChallenge')", "Local intranet", and a progress indicator.

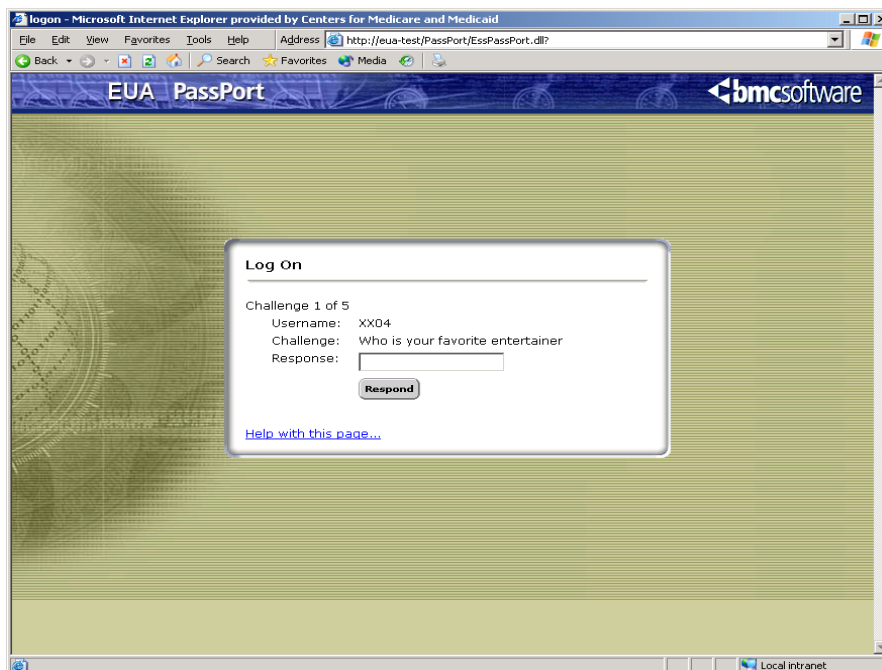
To set up the challenge, the user types and retypes the response, and selects “Apply Changes”. Responses need to be provided for all challenges. They must be a minimum of 4 characters, and the same response cannot be used for more than one challenge.

## Logging on to PassPort Without a Password

Once the challenges and responses have been set up, the user can access PassPort without a password. This is done by selecting “Log on without your password” in the initial PassPort login screen:



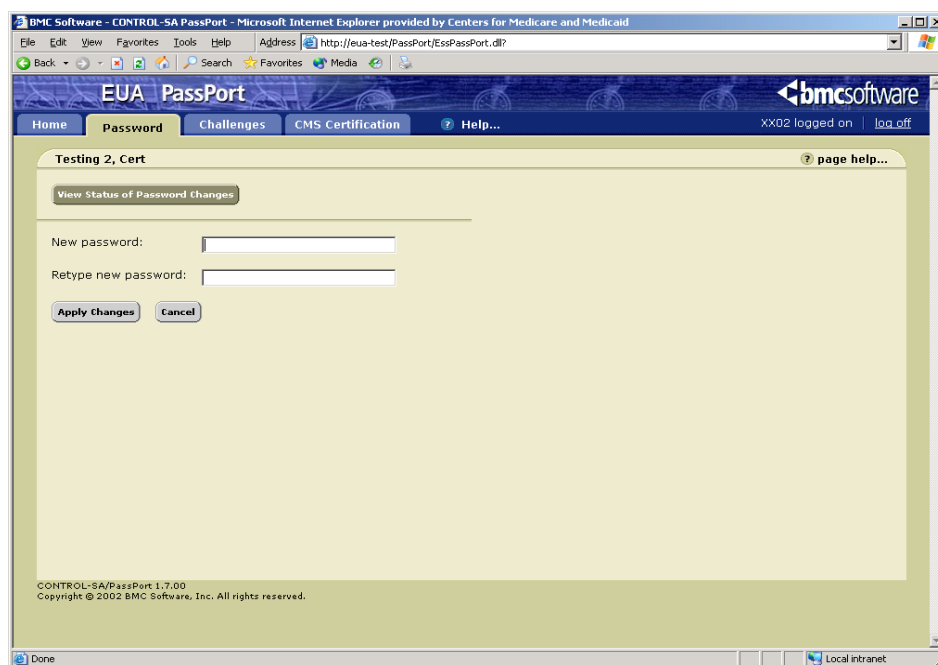
The user will be asked to provide responses to five randomly selected challenges:





## EUA Users Guide

When all five are answered correctly, the user is allowed to access PassPort. At this time, the password can be changed by selecting the Password tab:



Upon completion of the password change, all user accounts are restored with the new password, and the password is valid for 60 days.

### Revision History:

6/01/2004	Version 1.0
10/26/04	Version 1.1 – Privacy Act screen